Policy and Internet

PSO

Any Thing for Anyone? A New Digital Divide in Internet-of-Things Skills

Alexander J. A. M. van Deursen and Karen Mossberger

The "Internet-of-Things" (IoT) promises social benefits across a range of policy areas, such as energy, health, transportation, public safety, and environmental policy, but attention to the skills needed by individuals who use it will be an important issue for public policy, in order to ensure full exploitation of these technologies and to avoid unintended consequences. We argue that comparative advantages of the IoT to people will vary based on differentiated skills and resources, enabling smaller groups of people to benefit, and disadvantaging others in new ways. This need for renewed attention to digital skills and knowledge might at first seem paradoxical, given that many of these technologies operate autonomously and behind the scenes. We discuss evolving digital technologies and related skills, and explain from a systems perspective how the IoT differs from prior technologies, with a premium placed on user knowledge and strategic skills. Finally, we bring together the issues of the digital divide and IoT skills, and set an agenda for future IoT public policy and research.

KEY WORDS: Internet-of-Things, IoT, digital skills, digital divide, big data, public policy

物联网(Internet - of - Things， IoT)承诺为一系列政策领域带来社会利益， 这些领域包括能源、卫生、运输、公共安全和环境政策。但对于使用物联网的个人而言，他们所需技能的关注度将会是公共政策的一项重要议题， 因为要确保这些技术的完全使用， 同时避免产生意料之外的后果。本文主张，基于不同技能和资源，IoT给人们带来的比较优势也会有所不同，从而使得较少的人群获利， 同时以新的方式给其他人带来不利。考虑到许多技术都是在幕后独立操作，使得人们重新关注这些数字技术和知识在一开始看来显得比较矛盾。本文讨论了不断发展的数字技术以及相关技能， 同时从系统的视角解释了IoT如何与先前技术存在不同， 并着重提到了用户知识和策略技巧。最后， 本文将有关数字鸿沟和IoT的议题汇集在一起， 并设置议题用于未来IoT公共政策和研究。

关键词： 物联网，IoT，数字技能，数字鸿沟，大数据，公共政策

El "Internet-of-Things" (IoT) promete beneficios sociales en un rango de áreas de la política, como la energía, la salud, el transporte, la seguridad pública y la política ambiental, pero la atención a las habilidades que los individuos necesitan para usarlo será un tema importante para la política pública, para poder asegurar una explotación completa de estas tecnologías, y así´ evitar consecuencias no deseadas. Argumentamos que las ventajas comparativas del IoT para la gente serán diferentes dependiendo de las diferentes habilidades y recursos, permitiéndole a los grupos más

doi: 10.1002/poi3.171

pequeños de personas beneficiarse y desfavoreciendo a otros de nuevas maneras. Esta necesidad de atención renovada a habilidades digitales y conocimiento podría ser paradójica al principio, dado que muchas de estas tecnologías operan de forma independiente y en segundo plano. Discutimos las tecnologías digitales que están evolucionando y las habilidades relacionadas, y explicamos desde una perspectiva de sistemas cómo el IoT difiere de tecnologías anteriores, con una atención especial al conocimiento de los usuarios y las habilidades estratégicas. Finalmente, juntamos estos temas de la brecha digital y las habilidades del IoT, y establecemos una agenda para las políticas e investigación del IoT en el futuro.

PALABRAS CLAVES: Internet-of-Things, IoT, habilidades digitales, brecha digital, macrodatos, políticas públicas

Introduction

Declining wages, financial handouts to banks, austerity programs in social spending, and the transfer of the tax burden to wages are all commonly cited reasons for the recent growth of social inequality in the West (OECD, 2015). Given the vast body of literature on the digital divide—which usually studies how different social groups access technology—it is remarkable that the role of technology is rarely mentioned in political discussions about social inequality. Although information technology has assumed a secure place today in the civilized life and prevailing standards of contemporary society (Mossberger, Tolbert, & McNeal, 2008), technology and social processes often remain separated in policy (Robinson et al., 2015). Just as education has promoted democracy and economic growth, the Internet has the potential to benefit society as a whole, facilitating the membership and participation of individuals within society (Mossberger et al., 2008). Yet, policies to account for one's participation in society online need to address several societal groups, all with their own challenges, as digital divide research shows.

Early research concerning the digital divide primarily considered a twofold classification: "haves" versus "have nots." Now, digital divide research applies multifaceted conceptualizations, spanning motivation, material access, skills, use, and outcomes. In general, digital skills are considered the primary requirement for conducting capital-enhancing activities online, for obtaining positive outcomes from Internet use, and for the entire process of access and information inequality (van Dijk & van Deursen, 2014); consequently, they are deeply entwined with the notion of the digital divide (Livingstone & Helsper, 2010). From this viewpoint, it is crucial to look at the latest phase of technological development, that of the Internet-of-Things (IoT). The IoT comprises everyday devices implemented with microprocessors and sensors beyond the rectangular confines of personal computers (PCs), laptops, tablets, and smartphones. The technology has been finding wide applicability and is expected to deliver great benefits to its users (Atzori, Iera, & Morabito, 2010; Gubbi, Buyya, Marusic, & Palaniswami, 2013).

Many of the possibilities enabled by the IoT that are emphasized in popular media are techno-utopian promises that stress the autonomous power of the technology. However, deterministic promises often fail to achieve the predicted positive effects (Bibri, 2015). One important reason is the lack of skills needed to fully exploit technologies, or to avoid problems. There has been rapid evolution of the Internet, but little discussion of how this affects the skills needed for individuals, and the role of public policy to account for different skill levels. In this article, we will argue that the IoT phase of technological development requires renewed attention to digital skills—paradoxically, given that many of these technologies operate autonomously and behind the scene. We expect comparative advantages for areas such as health and energy cost savings to increase based on differentiated skills and resources, enabling smaller groups of people to benefit, and disadvantaging others in new ways. We propose an agenda for further research on IoT, skills and implications for public policy.

We discuss the development of the Internet into the IoT, and provide a working definition. We show how skills demands have developed with technological changes and what this means for IoT and public policy. We then discuss the implications that the need for IoT-savvy skills has for widening social disparities. Following this, we reflect on public policies that can enable more widespread levels of awareness and skills for the IoT. Finally, we bring together the digital divide and IoT skills, and set a possible agenda for further research and analysis.

Defining the IoT

Digital technologies have evolved rapidly over the past several decades, and will continue to grow in their capabilities, changing the way that end users interact with technologies, and the skill sets needed by individuals. The development of the Internet transformed the uses for the PC, building a network of computer networks. Web 1.0 drastically changed the way in which individuals and organizations searched for and used information. Web 2.0 allowed users to read, but also write, modify, and update content, increasing levels of user participation. Web 3.0 is a term linked to the semantic Web, which promises improved search and data sharing (Nath, Dhar, & Basishtha, 2014).

The impact of the Web goes far beyond its use for interpersonal communication and information sharing, particularly with the rapid development of the IoT. Advances in technology are once again changing the way in which end users interact with digital technologies. In the vision of the IoT, an increasing number of embedded devices of all sorts are capable of communicating and sharing data over the Internet (Zeng, Guo, & Cheng, 2011). A recent trend is to view IoT as the "Web of Things" in which open Web standards are supported for information sharing and device interoperation (Zeng et al., 2011). By penetrating smart things into the Web, conventional services can be enriched with physical world services. Although there is no generally accepted definition of the IoT (Whitmore, Agarwal, & Da Xu, 2015), existing notions do agree on several aspects (e.g., Atzori et al., 2010; Gubbi et al., 2013; Perera, Zaslavsky, Christen, & Georgakopoulos, 2014). Based on these commonalities, for the purposes of the discussion in this article we consider IoT as:

Systems that:

- contain *ubiquitous "everyday" objects* (e.g., mobile phones, smoke detectors, cars, wearables, home appliances, etc.) that are accessible through the Internet and equipped with *sensing, storing, and processing capabilities* that allow these objects to *understand their environments;*
- contain *identifying and networking capabilities* that allow them to *communicate information about themselves;*
- involve *object–object, object–person, and person–person communication;*
- and make autonomous decisions.

Examples of the IoT include: Personal items such as glasses, medical devices, and wearables (from fitness trackers to baby socks); the smart home (e.g., digital assistants such as Google Home, smart thermostats, boilers, light bulbs, home security, fridges, televisions, etc.), connected car systems (evolving into autonomous vehicles), and smart communities where electricity grids, traffic systems, and street lights incorporate sensors and collect data continuously. There are many potential benefits. Smart devices can empower individuals through information—with data that helps them to make better decisions about, for example, energy usage or health practices. Additionally, the production of big data from the many sensors and devices is a public good that can be used by policymakers for critical decisions, for example concerning disease control, environmental monitoring, or transport planning. Yet, the ability to realize these potential benefits depends in part on the knowledge, skills, and informed use of the individuals using it, and appropriate public policies to foster greater transparency and control of information, and to safeguard privacy and security. This is not a simple undertaking. The IoT is much more complex and abstract than previous information and communication technologies (Johnson, Adams Becker, Estrada, & Freeman, 2015). There are many connections occurring within the IoT, with user–device interfaces, devices communicating with other devices, third-party organizations (often unknown to the individual), and the reactions of both individuals and these entities to the data. Several features of the IoT present new challenges for users in comparison with previous waves of Internet use. These include:

More Data (e.g., Atzori et al., 2010; Perera et al., 2014; Riggins & Wamba, 2015). The ubiquity of devices has vastly increased the amount of data being collected in "large, diverse, complex, longitudinal, and/or distributed data sets generated from instruments, sensors, Internet transactions, email, video, click streams, and/or all other digital sources available today and in the future" (National Science Foundation, 2012, p. 5). While big data has been referred to as transformative, there are concerns about privacy and discriminatory uses (e.g., Tene & Polonetsky, 2012; White House, 2016).

Less Autonomy (e.g., Friedewald & Raabe, 2011; Pereira, Benessia, & Curvelo, 2013). Decisions are made automatically behind the scenes, based on data and algorithms. From refrigerators that generate shopping lists to autonomous vehicles that navigate traffic, IoT devices are replacing human actions, judgments, and decisions. Devices communicate information automatically, so there may be few, if any, decision points for intervening, including for controlling third-party access to data. As more decisions are surrendered to devices in our homes and communities, we may be oblivious to biases within these systems. These include the promotion of consumerism (such as the ease of ordering from Amazon through Echo). Health wearables, connected cars, and smart grids are designed in part to provide feedback to "nudge" us toward decisions that make us better off, by our own assessments (Thaler & Sunstein, 2008, p. 5). Institutions can also use such data, however, to penalize individuals, diminishing their autonomy rather than merely influencing the decision context.

Less Visibility and More Ambiguity (e.g., Pereira et al., 2013; Rainie & Anderson, 2017a). Technology use in the IoT occurs in a larger social system. This generates "dynamic complexity" (Sterman, 2006) where there is interdependence and constant evolution of the system. Unintended consequences may develop through uses of data and decisions that are made either autonomously through devices or by organizations, which may be distant from the individual and difficult to observe (Sterman, 2006). IoT systems consist of more than interconnected devices, but also involve different organizations or stakeholders, with multiple goals, which may conflict (Meadows & Wright, 2008)—for example, individuals who offer information to understand their own health, hospitals that use the data for research, and insurance providers who wish to lower their costs. Individuals may not be aware of data collection, for example, with sensors used in smart streetlights, let alone able to predict resulting consequences. The data and algorithms that form the basis of the IoT operate largely as a black box, where the quality of data or the assumptions behind algorithms are not transparent (Rainie & Anderson, 2017a).

More Risk (e.g., Sicari, Rizzardi, Grieco, & Coen-Porisini, 2015; Ziegeldorf, Morchon, & Wehrle, 2014). Online security and privacy risks are magnified by the IoT, with the proliferation of connected devices providing more entryways for security risks such as cyberattacks and denial of service attacks (FTC, 2015; Internet Society [IS], 2015). Security measures vary and may not be built into low-cost devices; there is also a threat that unencrypted data can be intercepted by unauthorized users. Because of the interconnected nature of the IoT, any poorly connected device can jeopardize the security of networks (IS, 2015). More generally, the production of vast amounts of data call into question a number of privacy issues. The complexity and lack of visibility in IoT systems mean that users may not know what data are being collected, how it is being used, and with whom it is being shared. Because of the diversity of data that are collected, it is

> possible to connect multiple streams of data to create a detailed profile of habits, demographics, and well-being (FTC, 2015; IS, 2015). Such information could possibly be used to impact credit, employment, or insurability, as well as for criminal purposes (FTC, 2015).

The skills implications for the IoT warrant closer examination and further research to support effective policy, minimize harms, and maximize the social benefits from these innovations.

Changing Technology, Changing Skills

To demonstrate how skills have changed with technological advancements, we focus on a typology of skills developed by van Dijk and van Deursen (2014). They distinguished between skills that can be applied to offline and online media:

- Operational skills, required to command media.
- Formal skills, required to use the formal characteristics of media (e.g., chapters, a book's table of contents, television channels, and online hyperlinks).
- Information skills, required to search, select, process, and evaluate information.
- Communication skills, required to decode and encode messages, exchange meaning, manage contacts, and attract attention.
- Content creation skills, required to create content of acceptable quality (e.g., text, photos).
- Strategic skills, required to use (digital) media as a means for personal or professional goals and to improve one's position in society.

van Dijk and van Deursen (2014) consider the primary operational skills for using computers to be the ability to read and write and to use audiovisual media. Additional skills are needed for the operation of hardware and software. The formal skills for using computers also differ from those required to understand the organization of print or audiovisual media, since information is contained in drives, folders, and files. The development of the PC, therefore, emphasized new sets of operational and formal skills for media use, albeit built on prior foundations such as basic literacy. The advent of Web 1.0 added operational skills to use an Internet browser and numerous apps, and formal skills to adequately use hypermedia in which users can choose their own nonlinear paths, providing substantial user control. The most dramatic change was the increased need for information skills for searching, selecting, processing, and evaluating information, including digital texts, images, videos, and figures. This has elsewhere been referred to as "information literacy" (Calzada Prado & Marzal, 2013; Mossberger, Tolbert, & Stansbury, 2003), for it requires higher-order skills than basic literacy, including problem solving and critical thinking about the legitimacy of sources. Information skills required for traditional media are similar to those needed for the Internet. The difference is that the information provided by the Internet is virtually infinite. Furthermore, the greater diversity of sources places much more pressure on information skills such as the assessment of credibility. Finally, strategic skills require users to make distinctions between goals and means and between what is more and less important to reach these goals. In order to acquire strategic skills, users have to be critical, analytical, and have a high degree of information skills (van Dijk & van Deursen, 2014).

The Internet also demanded different communication skills, first through email, listservs, and chat rooms in Web 1.0, and later through social media in Web 2.0. Both necessitated learning to communicate in online or virtual environments with the reduction of nonverbal behavior cues. More complex systems of networked communications call for social and collaborative skills online. Social media also differ in their purposes and audiences across platforms, involving choices and strategic skills. In the context of Web 2.0, content creation skills have become increasingly important. Online platforms allow users to post content without html knowledge, democratizing content online, but also substituting communication skills for operational ones. And, as open data portals have proliferated, allowing users to view and interact with data through visualization, downloading, or the creation of apps, Web 2.0 has escalated needs for data literacy as an information skill. Data literacy are "a component of information literacy that enables individuals to access, interpret, critically assess, manage, handle, and ethically use data" (Calzada Prado & Marzal, 2013, p. 126).

The examples above show that while the type of skills remain similar for different phases of technology development, the needed skills have acquired a different meaning or emphasis over time. Some changes in technology lower certain skill requirements—for example, searches that become easier with natural language processing, and social media features that substitute for knowledge of html. As compared to traditional media, van Dijk and van Deursen (2014) argue that on the one hand, computers and the Internet have made things easier, because they enable systematic, simultaneous information retrieval from innumerable sources. However, they also stress that information seeking and benefiting from media has become more difficult because it assumes new operational and formal skills, as well as greater information literacy. Recent work on the popular notion of 21st century (digital) skills comes to this conclusion as well; besides information and communication, there are greater requirements for problem solving, critical thinking, and creativity (van Laar, van Deursen, van Dijk, & de Haan, 2017). Likewise, there are certain skills that are emphasized in the IoT, as well as others that become less relevant.

The IoT: The Paradox of Skills

In order to illustrate the skills needed to use the IoT from a user's perspective, Table 1 shows how five features of the IoT may affect digital skills, increasing demands for some, while decreasing the need for others. Where spaces are left blank, we anticipate that there is little change, though these are empirical questions that need to be answered by further research.

Decreasing Need for Operational and Formal Skills

Table 1 reveals that two IoT characteristics limit the stress on operational and formal skills, such as the ability to use hardware and software. There are operational and formal skills involved in initial set-up or control of settings on some devices, but the IoT differs from traditional technologies that are characterized by continuous user–device interaction. Furthermore, other devices are embedded in the environment, with little control possible on the part of individuals. Overall, operational and formal skills in the IoT are less frequent and less visible. Because the IoT comprises sensing, storing, processing, identifying, and networking capabilities embedded in ubiquitous "everyday" objects, the technology can integrate itself into everyday life and become indistinguishable from it. From this point of view, one might argue that the IoT will simplify our lives because it is characterized by ease of use: It works automatically and unnoticed, limiting the importance of operational and formal skills.

Example: Smart thermostats have access to calendars, beds, and cars, and can plan heating and cooling based on the location of the house's occupants. The sensing and data processing occurs invisibly to the user. When you leave the house, the smart thermostat will automatically turn off devices. There is little need for operative actions.

Second, users have less autonomy. The objects in the IoT system sense their environments and communicate with other devices and people. All devices and persons involved create a complex, omnipresent system in which IoT devices not only go unnoticed, they also make autonomous decisions to help users deal with the huge amount of ambiguous data. From a user perspective, this will lead to less autonomy: The IoT system decreases decision points where operational and formal skills are applied. Whereas previous technologies typically required a fully aware user to operate a device, in the IoT, humans can be mostly passive and unaware of what is happening.

Example: Autonomous vehicles greatly reduce the need for driving skills. Driving decisions made autonomously by the vehicle are based on collected data concerning aspects such as road conditions or another car's actions. As a result, the driver requires limited operational skills.

Table 1. IoT Characteristics and Potential Effects on Needed Skills

	Less Visibility	Less Autonomy	More Data	More Ambiguity	More Risk
Operational	–	–			
Formal	–	–			
Information			+	+	+
Communication			+?	+?	+?
Strategic			+	+	+

Increasing and Changing Needs for Information, Communication, and Strategic Skills

Table 1 reveals three IoT characteristics that increase the importance of information, communication, and strategic skills. First, the IoT system generates more data as compared to prior technologies through its sensing, storing, and processing capabilities. Strategic skills are required to decide what sort of data the IoT system is going to collect and how and why this data will be analyzed, applied, and shared. Increasingly, users will need to utilize detailed information generated by the IoT's appliances. Information skills are required to visualize the data in an understandable format (Barnaghi, Wang, Henson, & Taylor, 2012) and to interpret the massive amount of collected data. Communication skills are required to share the data, for example, to compare these with data of other users, and extract meaning from other users' comments and opinions. Communicating about data in the IoT demands different types of skill in comparison with communication skills needed for Web 2.0 features such as social media. This may be a case of changing skills rather than a clear increase in skill, however.

> *Example: Turning on a health wearable automatically results in a large collection of physiological and environment data. This enables the device to track day-to-day activities (e.g., walking pace, floors climbed, locations visited), and measure health parameters (e.g., blood pressure, heart rate, stress level, breathing activity). Software will aggregate data, but the user must understand how it is used and applied. This requires data visualization, interpretation, and evaluation, and possibly the sharing of data for comparisons and strategic decision making. Knowledge on how data is shared is required since the collected data reveals how often a person exercises, how they travel to work, or potential illnesses. Such intimate information could be of interest to (insurance) companies, creditors, and law enforcement.*

The amount of data are not only increasing, it is also becoming more complex and ambiguous as it is the result of sensing and object–object, object–person, and person–person communication. The complexity and dynamics of IoT scenarios require a distribution of intelligence in the IoT system, making smart objects able to react autonomously to a wide range of different situations (the idea behind the IoT is to help people master the complexity involved). As a consequence of the easy transformation from one system entity into another, we can expect problems identifying who has the data, and system boundaries (Popescul & Georgescu, 2014). As a result, for users it will be hard to understand the rationale governing the interactions involved in the IoT system in which multiple persons and devices located in different contexts exchange information. Whereas previous technologies typically required a fully aware user to operate a device, in the IoT, humans can be unaware of what is happening. For example, a malfunctioning connected vehicle that does not correctly record braking behavior could impact insurance rates, though the driver may not understand that inaccurate data are being generated and its implications. For users it will be increasingly difficult to reason about possible device interactions and their effects, leading to incomplete specifications and misinterpretation. Without the ability to interpret, analyze, check, and communicate data correctly, users may end up collecting wrong data, ignoring the right data, failing to apply the data (correctly), or extracting the wrong meaning from it. As a result, there will be much more emphasis on information skills (selection, interpretation, and quality assessment), communication skills (understanding how devices communicate with other devices and humans and vice versa, and how users communicate with other users in the IoT system), and strategic skills (deciding what data should be collected and how it should be used to gain optimal outcomes).

> *Example: Health wearables provide numerous parameters and might lead to the conclusion that a user often shows high stress levels. Since there are different ways to interpret the presented data, there may be no clear solution. The system does not tell the user who or what is triggering the stress. The user needs to critically evaluate how the data is collected and what the conclusion is based on. Yet, because the system has warned the user of increased stress levels, (s)he has a greater responsibility for responding through preventive measures. Furthermore, the increased stress levels might trigger interventions by doctors without complete information about the context. As a result, your doctor may tell you to take medication (which may be helpful, though it could also lead to overmedication when other solutions would have been more effective) and your insurance provider may increase your premium because of increased risks (not so helpful). In this case, individuals need to understand the information that is being generated, and communicate with others in the system to provide additional information or to advocate on their own behalf.*

Finally, the management of risk is critical for the IoT, yet also more difficult than with previous technologies. The U.S. National Intelligence Council (2008, p. 27) stresses that "to the extent that everyday objects become information security risks, the IoT could distribute those risks far more widely than the Internet has to date." Trust, privacy, and security management are increasingly imperiled when automatic communication between IoT objects is deployed (Atzori et al., 2010). Because IoT technology works in the background the risks that accompany IoT use are often not obvious to users. IoT devices, for example, can unknowingly be triggered to reply with their ID and other information. Security is one concern, with hacking of connected baby monitors, locks, cars, and medical implants such as pacemakers posing clear dangers (FTC, 2015; Rainie & Anderson, 2017b). Additionally, the collection, analysis, and use of data are often not transparent to users, making it more difficult to make strategic decisions about whether or not to use a device, because of the risks compared to the benefits.

> *Example: The IoT can enable the adaptation of a room's heating to either personal preferences or weather. Skills are required to decide how the collected data will be used. These data potentially reveal when a person is home and how often he or she*

> *cooks, showers, watches television, or exercises. Such intimate information will be considered private by many but if he or she is not able to protect data sharing or comprehend the identity of the involved mediators, (insurance) companies, creditors, and law enforcement, might use it to their own benefit. Even more harm can be done when such detailed information falls in the hands of criminals.*

Risks are even more unclear when individuals are not the adopters of devices, for example, when they are exposed to sensors that collect data on their movements in traffic or drones surveilling their neighborhoods. Despite the social benefits for intelligent traffic systems and environmental sensors, increased monitoring and data collection may also have implications for privacy and civil liberties (White House, 2016). Information skills can help individuals to understand possible risks of the connected environment, though strategic decisions may be difficult in this context.

In the IoT, links between devices, actors, and purposes are often concealed. For the ordinary user, it can be difficult to comprehend whether they can trust security measures or even the identity of the mediators and the identity of who controls the data. Consequently, IoT interventions can be unintended, unforeseen, and unexpected. In the next section, we discuss the need for individual skills and for public policies that compensate for the limits of individual skill.

Skills and Public Policy

Characteristics such as less visibility, less user autonomy, increased data, ambiguity, and risk require users to have the skills to assess potential outcomes of their IoT use. Users should be able to take appropriate actions to increase benefits, protect privacy and mitigate risks, and to be assured that privacy and security are enforced beyond their immediate sphere of control (Ziegeldorf et al., 2014). This entails the information skills to ask the right questions and find the answers before adopting IoT technology. What information is being collected, and who will have access to it? Will this help to improve the product, or provide a public good, supporting research or better services? If information will be shared with third parties, what will be the limits on that sharing? Will data be secured through encryption? Will it be de-identified, and used only in the aggregate? What security is embedded in a device, and is it updated by the manufacturer? Are there strong authentication systems? With respect to user's skills toward technology, producers and public authorities can have conflicting interests. While producers of IoT may like passive users who accept standard settings, public authorities might strive toward fostering the availability of such information and enable individuals to make strategic decisions. There are a number of ways in which individuals can be given more information and choice. Notice and consent, for example, is required for sharing locations on smartphones, and can be used in some instances for the IoT. But what about devices that do not have a screen or user interface? Informed consent and/or the ability to manage privacy settings can occur at the point of purchase or when individuals agree to participate in a service. Organizations that promote IoT use, such as health care providers or insurance companies, are points of contact where notice and consent can occur. Manufacturers can maintain websites with information that is clear and easy to understand (FTC, 2015). In public settings, where citizens have less individual control over use, local governments can engage citizens in collective discussions about the privacy and security implications of smart city innovations.

Moreover, Howard (2015) argues that the need to build new institutions for governing the IoT requires civic engagement. Such processes both contribute to and rely on the digital skills of individual citizens. Industry has some incentives to improve security and offer alternatives for privacy, in order to promote consumer confidence. But, this also depends on consumers who have the information, communication, and strategic skills to be discerning customers. The media and educational systems clearly have a role to play in promoting digital skills for consumer decisions and civic engagement. Nonprofit organizations (such as the Electronic Frontier Foundation) that publish ratings on digital privacy or security could also be helpful in creating greater transparency and public pressure for trustworthy practices (Fung, Graham, & Weil, 2007). As research on voluntary regulation demonstrates, self-policing is most likely to be effective where there is visibility and scrutiny, and in situations where industries anticipate that governments will impose regulations if businesses do not (Hsueh, 2013). Debates over future IoT regulation are emerging in national governments and international bodies (EC, 2017; FTC, 2015), as policy attempts to catch up with the development of technology.

While public policies and business practices are needed for greater transparency, the success of such policies will demand greater levels of skill as well; users will need to apply information skills to assess the sensitivity of the data collected, communication skills to discuss potential privacy concerns, and strategic skills in order to make access control decisions.

IoT Skills in the Digital Divide Debate

Recent investigations in western societies suggest that although an increasing number of people have access to the Internet, inequality continues to rise on account of skills and usage opportunities (for a review of determinants, see Scheerder, van Deursen & van Dijk, 2017). In the contemporary literature on the digital divide, inequality of Internet skills is acknowledged as a key dimension, affecting types of engagement and social outcomes of Internet use, or digital citizenship (Mossberger et al., 2008). While there is evidence regarding the benefits of Internet use for economic opportunity, civic engagement, and political participation (Boulianne, 2009; DiMaggio & Bonikowski, 2008; Mossberger et al., 2008), these gains are not equal across all Internet users. Technologies offer more capital-enhancing opportunities for those of higher socioeconomic status (DiMaggio & Garip, 2012; Robinson et al., 2015; Sparks, 2014).

Given how the conceptualization of the digital divide is evolving with the IoT system, we argue that there is a strong need to incorporate the IoT in digital divide research: Identifying populations which will be most affected and how public policy can address any resulting disadvantage. Popescul and Georgescu (2014) debate whether a fair distribution of benefits and costs—as well as equal opportunities in gaining advantage from the IoT—are possible. The complex nature of the IoT demands greater attention to these outcomes, including the distribution of costs and benefits, rather than the traditional focus primarily on adoption or uses. Skills remain a key linkage between use and outcomes.

As we have seen, the IoT requires a high level of information, communication, and strategic skills. Performance tests conducted in the Netherlands showed that subjects had a high level of operational Internet skills but struggled with information and strategic skills (van Deursen & van Dijk, 2009, 2011). Education is an important resource for these skills, and its significance will increase for information skills like data literacy, and the ability to make strategic choices to protect privacy and security. A recent survey showed that respondents with a high school education or less averaged only 4 out of 13 correct responses on cybersecurity questions, compared to 7 out of 13 for college graduates (Olmstead & Smith, 2017). These results call into question whether many people will have the capacity to understand what is happening in complex IoT systems, including who owns the data they generate and what decisions are made based on those data. IoT has a potentially consequential impact for people with different levels of resources and power (e.g., it affects hospital treatment, medication intake, insurance allowance, and energy consumption). Those who depend on institutional services because of disability, health, or low incomes may be those who are most vulnerable to abuses in the IoT, because they are likely to possess the lowest skill levels. To the extent that smart city solutions address issues such as environmental quality or public safety, low-income communities may be at the forefront of deployment, but also least prepared to participate in representing their interests or protecting themselves from discrimination or surveillance.

Additionally, the IoT can deepen inequalities through big data, in areas such as hiring, credit, insurance, health care, and service access. Nonrepresentative data that excludes racial and ethnic groups, women, the disabled, the elderly, and the poor reinforces existing biases, with a veneer of objectivity (O'Neil, 2016). The algorithms that drive the IoT have values and assumptions embedded within them, which must be examined critically. Experts canvassed by the Pew Research Center have argued that currently "those who create and evolve algorithms are not held accountable to society" (Rainie & Anderson, 2017a, p. 74) and that there is a need for transparency and oversight, as well as greater algorithmic literacy in the population and ethical training for those who create the codes.

Toward a Research Agenda on the IoT and Skills

In addition to the relationships between IoT characteristics and skills discussed in Table 1, there are many questions to explore regarding the IoT. To obtain a thorough understanding of IoT skills inequality in daily life, we suggest scholars should fuse knowledge from different disciplines to:

- Go beyond both the common technical approach to studying the IoT and the technological deterministic perspective that often characterizes research on digital inequality (Tsatsou, 2014). In order for public policy to make the IoT more visible for the user, to give the user more autonomy, and to reduce the risks connected to IoT usage, we will need to account for individuals' skills and needs, their interactions with the IoT, and their relationships with others within relevant systems (including the distribution of power).
- Investigate the IoT on a systemic level. One of the challenges for understanding skills and inequality in the IoT is that the term represents a general concept that encompasses many "things." Given applications with varying levels of visibility, autonomy, data, ambiguity, risks, and benefits, more investigations of the characteristics and dynamics of the systems surrounding these applications will need to be undertaken. Mapping systems across applications and policy areas and categorizing them along these or other variables could be a first step in theorizing about different applications and studying the required skills.
- Study whether the IoT characteristics discussed affect the skills in the way outlined in this article.
- Develop scales to understand the needs of individuals and the contexts in which they learn and apply their skills. At the individual level, we need to understand the experiences, perceptions, and attitudes of those who are engaged (or not) with different IoT applications, including individuals of varied social backgrounds. How do they understand their interactions with the IoT? How do they perceive the costs and benefits? To what extent do they make choices about participation? How much do they use and benefit from data produced by the IoT?
- Take a social contextual approach to inequality in order to explain differences in IoT skill levels. van Dijk (2005) argues for a relational approach, focusing both on individuals' positions and the positions between them (Wellman & Berkowitz, 1988). For example, instead of arguing that a more highly educated man is more skilled at using the IoT than a less highly educated man, a relational view might reveal that the highly educated man receives more stimulation from the people around him. The "rich get richer" model (Kraut et al., 2002) predicts that those who have social support will obtain additional social benefits from their Internet use. Learning IoT skills in the home context might be less beneficial for the people with the greatest need for IoT skill improvements (van Dijk & van Deursen, 2014). Children from poor families and families with low education levels may not receive adequate support from their parents and siblings, whereas children from wealthy and highly educated families may receive support from parents, homework assistants, siblings, or others who are Internet savvy. Besides the importance of others, the development of skills is explained by one's family's cultural capital (Bourdieu, 1986). This may or may not be intentionally transmitted by family practices of support.

- Explore the social context for developing IoT skills at different scales. Although a variety of studies on information and communication technologies highlight the importance of one's surroundings and informal social networks (e.g., Fulk, 1993; Stewart & Hyysalo, 2008), the role played by social networks, households, communities, and public institutions in facilitating the use of IoT skills is unknown. Scales explored should be household interactions with the technologies, environments in local communities, and the effects of national institutions (such as regulatory regimes) across countries. Communities are important venues for research, to understand both local support systems and also systemic interactions beyond individuals and households. Prior research on technology use suggests that the user is supported by developing knowledge within a community setting, helping both reinterpret and develop experiences (Pinkett, 2000). Digital skills are strongly shaped by the local social context (Ferro, Helbig, & Gil-Garcia, 2011), including by neighborhood influences such as poverty and segregation (Mossberger, Tolbert, & Hamilton, 2012) and institutions such as schools and media.
- Apply multiple methodological approaches. There are several data-collection methods that can be employed to conduct a detailed investigation of how IoT skills are applied and learned. For example, combining IoT log data (e.g., a smart thermostat that provides energy history data) with qualitative methods (e.g., interviews) and quantitative (survey) methods. This way, IoT technologies not only are an object of study, but are also used to augment traditional methods of data collection, opening pathways for future studies in concrete social contexts.

A better understanding of individual skills within social contexts and technological systems could contribute to better outcomes for IoT use. Such research could inform changes in devices, education, and public policy that increase the benefits of IoT, and that empower users. Audiences include:

- IoT developers, firms, and other institutions employing IoT technology, to help them more effectively design usable and comprehensible IoT, with safeguards for privacy and security. Understanding what the IoT does for the user, how it fits into their lives and what experiences they have might result in improved instructions, support sites, help desks, etc. Better usability will reduce demand for technical skills, whereas improved comprehensibility will reduce higher-order skills requirements.
- Educators and trainers, to help them consider IoT skills in the educational field, libraries, and community-based organizations. We need to go beyond a technical perspective on IoT skills, necessary because the main educational policy worldwide has been to equip schools with technology (Selwyn, 2013). Educators and policymakers need to understand which skills are needed to participate in the IoT system and thus how to either adapt course programs and educational software or retrain teachers. The challenge is not only including IoT skills in the curriculum, but also understanding what capacities teachers need and the pedagogical practices that are most effective in developing IoT skills in students (Siddiq, Scherer, & Tondeur, 2016).

- Policymakers, to define targeted policies aimed at ensuring a more egalitarian society, and to provide the transparency and protections that are needed where individual action is insufficient. Because digital inequality is a critical issue in contemporary economy, we need to expand our understanding of how the IoT is employed among various sociocultural milieus. To close skill gaps, this suggests policies such as skills training, public information about the IoT, and regulations that require greater transparency and disclosure of how personal data are used. While there is concern that regulation will constrain innovation in some policy circles (FTC, 2015), the complexity and lack of visibility in IoT systems suggests a government role in promoting transparency as well as skill. Research can help to support evidence-based informational and regulatory solutions.

Conclusion

So far, behavioral factors that are necessary for understanding the impact of the IoT have been largely ignored (Riggins & Wamba, 2015) and the social sciences have not sufficiently contributed to the IoT's development (Atzori et al., 2010; Shakiba, Zavari, Aleebrahim, & Singh, 2016). Consequently, we know little about how individuals participate within IoT systems, and how this is affected by critical user skills. We have argued that the abstract and autonomous system that the IoT creates does not erase the need for skills. While stress on operational and formal skills might be reduced because of lower visibility and more autonomy of the technology, as a result of increased data volume, less user autonomy, more ambiguity, and more risks, there will be more stress on information, strategic, and certain communication skills to understand the uses and consequences of the IoT system.

While we have explored the use of IoT technology from the standpoint of the digital skills of individual users, the issue of skills raises a number of important questions for public policy and for further research. First, the IoT has many valuable applications across policy areas that are being pursued not only by private sector actors, but also by public institutions. This includes, most notably, local governments involved in the smart cities movement. Second, important potential benefits may also be accompanied by significant social costs. These include widening inequalities in digital citizenship, with users who are unable to take advantage of the data at their disposal, and who are less empowered to make decisions that are instead governed by unseen forces. Individuals may surrender their data and be penalized in unforeseen ways or suffer a loss of privacy. Both the benefits and the risks vary widely across the many possible applications of the IoT, and more research is needed to understand this variation, and how individuals and organizations interact in different IoT systems. Such research can help policymakers to address the skills that citizens need, and unintended consequences such as greater inequality or diminished privacy. Education and skills training, policies that promote information and transparency about the uses of data, better privacy and security practices in the industry, and regulation are options that may be considered in different instances, to facilitate potential benefits and reduce risks. More evidence in this emerging area is needed, and researchers can play an important role in examining skills, systems, and outcomes.

Dr. Alexander J. A. M. van Deursen, University of Twente, Enschede, Netherlands [a.j.a.m.vandeursen@utwente.nl].
Prof. Dr. Karen Mossberger, Arizona State University, Phoenix, Arizona.

References

Atzori, L., A. Iera, and G. Morabito. 2010. "The Internet of Things: A Survey." *Computer Networks* 54 (15): 2787–805.

Barnaghi, P., W. Wang, C. Henson, and K. Taylor. 2012. "Semantics for the Internet-of-Things: Early Progress and Back to the Future." *International Journal on Semantic Web and Information Systems* 8 (1): 1–21.

Bibri, S.E. 2015. *The Shaping of Ambient Intelligence and the Internet of Things*. Amsterdam: Atlantis Press.

Boulianne, S. 2009. "Does Internet Use Affect Engagement? A Meta-Analysis of Research." *Political Communication* 26 (2): 193–211.

Bourdieu, P. 1986. "The Forms of Capital." In *Handbook of Theory and Research for the Sociology of Education*, ed. J.G. Richardson. New York, NY: Greenwood Press, 241–58.

Calzada Prado, J., and M.Á. Marzal. 2013. "Incorporating Data Literacy Into Information Literacy Programs: Core Competencies and Contents." *Libri* 63 (2): 123–34.

DiMaggio, P., and B. Bonikowski. 2008. "Make Money Surfing the Web? The Impact of Internet Use on the Earnings of U.S. Workers." *American Sociological Review* 73 (2): 227–50.

DiMaggio, P., and F. Garip. 2012. "Network Effects and Social Inequality." *Annual Review of Sociology* 38: 93–118.

EC. 2017. *Internet of Things Privacy and Security Workshop*. https://ec.europa.eu/digital-single-market/en/news/internet-things-privacy-security-workshop.

Ferro, E., N.C. Helbig, and J.R. Gil-Garcia. 2011. "The Role of IT Literacy in Defining Digital Divide Policy Needs." *Government Information Quarterly* 28 (1): 3–10.

Friedewald, M., and O. Raabe. 2011. "Ubiquitous Computing: An Overview of Technology Impacts." *Telematics and Informatics* 28 (2): 55–65.

FTC. 2015. *Internet of Things: Privacy and Security in a Connected World*. January. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

Fulk, J. 1993. "Social Construction of Communication Technology." *Academy of Management* 36 (5): 921–50.

Fung, A., M. Graham, and D. Weil. 2007. *Full Disclosure: The Perils and Promise of Transparency*. Cambridge, MA: Cambridge University Press.

Gubbi, J., R. Buyya, S. Marusic, and M. Palaniswami. 2013. "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions." *Future Generation Computer Systems* 29 (7): 1645–60.

Howard, P.N. 2015. *Pax Technica: How the Internet of Things May Set Us Free or Lock Us Up*. New Haven, CT: Yale University Press.

Hsueh, L. 2013. "Beyond Regulations: Industry Voluntary Ban in Arsenic Use." *Journal of Environmental Management* 131: 435–46.

Internet Society. 2015. *The Internet of Things: An Overview. Understanding the Issues and Challenges of a More Connected World*. October. https://www.internetsociety.org/resources/doc/2015/iot-overview.

Johnson, L., S. Adams Becker, V. Estrada, and A. Freeman. 2015. *NMC Horizon Report: Higher Education Edition*. Austin, TX: The New Media Consortium.

Kraut, R., S. Kiesler, B. Boneva, J. Cummings, V. Helgeson, and A. Crawford. 2002. "Internet Paradox Revisited." *Journal of Social Issues* 58 (1): 49–74.

Livingstone, S., and E. Helsper. 2010. "Balancing Opportunities and Risks in Teenagers' Use of the Internet: The Role of Online Skills and Internet Self-Efficacy." *New Media & Society* 12 (2): 309–29.

Meadows, D.H., and D. Wright. 2008. *Thinking in Systems: A Primer*. White River Junction, VT: Chelsea Green Publishing Company.

Mossberger, K., C.J. Tolbert, and A. Hamilton. 2012. "Measuring Digital Citizenship: Mobile Access and Broadband." *International Journal of Communication* 6: 2492–528.

Mossberger, K., C.J. Tolbert, and M. Stansbury. 2003. *Virtual Inequality: Beyond the Digital Divide*. Washington, DC: Georgetown University Press.

Mossberger, K., C.J. Tolbert, and R.S. McNeal. 2008. *Digital Citizenship: The Internet, Society, and Participation*. Cambridge, MA: MIT Press.

Nath, K., S. Dhar, and S. Basishtha. 2014. "Web 1.0 to Web 3.0 - Evolution of the Web and Its Various Challenges." In *Optimization, Reliabilty, and Information Technology*. Haryana, India: IEEE ICROIT Conference, 86–9.

National Intelligence Council (NIC). 2008. "Disruptive Civil Technologies: Six Technologies With Potential Impacts on US Interests Out to 2025." Conference Report CR 2008-07. April. https://fas.org/irp/nic/disruptive.pdf.

National Science Foundation. 2012. *Solicitation 12–499: Core Techniques and Technologies for Advancing Big Data Science & Engineering*. http://www.nsf.gov/pubs/2012/nsf12499/nsf12499.pdf.

OECD. 2015. *In It Together: Why Less Inequality Benefits All*. Paris: OECD Publishing.

Olmstead, K., and A. Smith. 2017. "What the Public Knows About Cybersecurity." March 22. *Pew Research Center*. http://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity/.

O'Neil, C. 2016. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Crown Publishing Group.

Perera, C., A. Zaslavsky, P. Christen, and D. Georgakopoulos. 2014. "Context Aware Computing for the Internet of Things: A Survey." *IEEE Communications Surveys & Tutorials* 16 (1): 414–54.

Pereira, A.G., A. Benessia, and P. Curvelo. 2013. "Agency in the Internet of Things." European Commission Working Paper. http://publications.jrc.ec.europa.eu/repository/bitstream/111111111/30547/1/lbna26459enn.pdf.

Pinkett, R.D. 2000. "Bridging the Digital Divide: Sociocultural Constructionism and an Asset-Based Approach to Community Technology and Community Building." Paper presented at the 81st Annual Meeting of the American Educational Research Association April 24−28, New Orleans, LA.

Popescul, D., and M. Georgescu. 2014. "Internet-of-Things—Some Ethical Issues." *The USV Annals of Economics and Public Administration* 13 (2): 208–14.

Rainie, L., and J. Anderson. 2017a. "Code-Dependent: Pros and Cons of the Algorithm Age." February 8. *Pew Research Center*. http://www.pewinternet.org/2017/02/08/code-dependent-pros-and-cons-of-the-algorithm-age/.

Rainie, L., and J. Anderson. 2017b. "The Internet of Things Connectivity Binge: What Are the Implications?" June 6. *Pew Research Center*. http://www.pewinternet.org/2017/06/06/the-internet-of-things-connectivity-binge-what-are-the-implications/.

Riggins, F.J., and S.F. Wamba. 2015. "Research Directions on the Adoption, Usage, and Impact of the Internet of Things Through the Use of Big Data Analytics." In *System Sciences (HICSS), 48th Hawaii International Conference*. Kauai, Hawaii: IEEE, 1531–40.

Robinson, L., S.R. Cotten, H. Ono, A. Quan-Haase, G. Mesch, W. Chen, and M.J. Stern. 2015. "Digital Inequalities and Why They Matter." *Information, Communication & Society* 18 (5): 569–82.

Scheerder, A., A.J.A.M. van Deursen, and J.A.G.M. van Dijk. 2017. "Determinants of Internet Skills, Uses and Outcomes. A Systematic Review of the Second- and Third-Level Digital Divide." *Telematics and Informatics* 34: 1607–24.

Selwyn, N. 2013. "Empowering the World's Poorest Children? A Critical Examination of One Laptop Per Child." In *The Politics of Education and Technology*, eds. N. Selwyn and K. Facer. New York: Palgrave Macmillan, 101–25.

Shakiba, M., A. Zavari, N. Aleebrahim, and M.J. Singh. 2016. "Evaluating the Academic Trend of RFID Technology Based on SCI and SSCI Publications From 2001 to 2014." *Scientometrics* 109 (1): 591–614.

Sicari, S., A. Rizzardi, L. Grieco, and A. Coen-Porisini. 2015. "Security, Privacy and Trust in Internet of Things: The Road Ahead." *Computer Networks* 76: 146–64.

Siddiq, F., R. Scherer, and J. Tondeur. 2016. "Teachers' Emphasis on Developing Students' Digital Information and Communication Skills (TEDDICS): A New Construct in 21st Century Education." *Computers & Education* 92: 1–14.

Sparks, C. 2014. "Technological Innovation and Social Change." In *Technological Determinism and Social Change: Communication in a Tech-Mad World*, ed. J. Selwyn. London: Lexington Books, 65–86.

Sterman, J.D. 2006. "Learning From Evidence in a Complex World." *American Journal of Public Health* 96 (3): 505–14.

Stewart, J., and S. Hyysalo. 2008. "Intermediaries, Users and Social Learning in Technological Innovation." *International Journal of Innovation Management* 12 (3): 295–325.

Tene, O., and L. Polonetsky. 2012. "Big Data for All: Privacy and User Control in the Age of Analytics." *Northwestern Journal of Technology and Intellectual Property* 239: 1–36.

Thaler, R.H., and C.R. Sunstein. 2008. *Nudge: Improving Decisions About Health, Wealth and Happiness*. London: Penguin Books.

Tsatsou, P. 2014. *Internet Studies: Past, Present and Future Directions*. Surrey: Ashgate.

van Deursen, A.J.A.M., and J.A.G.M. van Dijk. 2009. "Using the Internet: Skill Related Problems in Users' Online Behavior." *Interacting with Computers* 21: 393–402.

van Deursen, A.J.A.M., and J.A.G.M. van Dijk. 2011. "Internet Skills and the Digital Divide." *New Media & Society* 13: 893–911.

van Dijk, J.A.G.M. 2005. *The Deepening Divide: Inequality in the Information Society*. Thousand Oaks: Sage.

van Dijk, J.A.G.M., and A.J.A.M. van Deursen. 2014. *Digital Skills, Unlocking the Information Society*. New York: Palgrave Macmillan.

van Laar, E., A.J.A.M. van Deursen, J.A.G.M. van Dijk, and J. de Haan. 2017. "The Relation Between 21st-Century Skills and Digital Skills: A Systematic Literature Review." *Computers in Human Behavior* 72: 577–88.

Wellman, B., and S.D. Berkowitz. 1988. *Social Structures: A Network Approach*. New York, NY: Cambridge University Press.

White House. 2016. *Big Data: Algorithmic Systems, Opportunity and Civil Rights*. https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf.

Whitmore, A., A. Agarwal, and L. Da Xu. 2015. "The Internet of Things—A Survey of Topics and Trends." *Information Systems Frontiers* 17 (2): 261–74.

Zeng, D., S. Guo, and Z. Cheng. 2011. "The Web of Things." *Journal of Communications* 6 (6): 424–38.

Ziegeldorf, J.H., O.G. Morchon, and K. Wehrle. 2014. "Privacy in the Internet of Things: Threats and Challenges." *Security and Communication Networks* 7 (12): 2728–42.